Ergodic Secret Alignment*

Raef Bassily Sennur Ulukus

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742

bassily@umd.edu *ulukus@umd.edu*

Abstract

In this paper, we introduce two new achievable schemes for the fading multiple access wiretap channel (MAC-WT). In the model that we consider, we assume that perfect knowledge of the state of all channels is available at all the nodes in a causal fashion. Our schemes use this knowledge together with the time varying nature of the channel model to align the interference from different users at the eavesdropper perfectly in a one-dimensional space while creating a higher dimensionality space for the interfering signals at the legitimate receiver hence allowing for better chance of recovery. While we achieve this alignment through signal scaling at the transmitters in our first scheme (scaling based alignment (SBA)), we let nature provide this alignment through the ergodicity of the channel coefficients in the second scheme (ergodic secret alignment (ESA)). For each scheme, we obtain the resulting achievable secrecy rate region. We show that the secrecy rates achieved by both schemes scale with SNR as $\frac{1}{2}\log(\text{SNR})$. Hence, we show the sub-optimality of the i.i.d. Gaussian signaling based schemes with and without cooperative jamming by showing that the secrecy rates achieved using i.i.d. Gaussian signaling with cooperative jamming do not scale with SNR. In addition, we introduce an improved version of our ESA scheme where we incorporate cooperative jamming to achieve higher secrecy rates. Moreover, we derive the necessary optimality conditions for the power control policy that maximizes the secrecy sum rate achievable by our ESA scheme when used solely and with cooperative jamming.

*This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127 and CCF 09-64645, and presented in part at the 47th Annual Allerton Conference on Communications, Control, and Computing, Monticello, IL, September 2009 [1], and the IEEE International Conference on Communications, Cape Town, South Africa, May 2010 [2].

1 Introduction

The notion of information theoretic secrecy was first introduced by Shannon in his seminal work [3]. Applying the notion of information theoretic secrecy to channel models with single transmitter, single receiver, and single eavesdropper (wiretapper) was pioneered by Wyner [4], Csiszar and Korner [5], and Leung-Yan-Cheong and Hellman [6]. Wyner [4], introduced the wiretap channel where it is assumed that the received signal by the eavesdropper is a degraded version of the signal received by the legitimate receiver. For his model, Wyner established the secrecy capacity region, which is defined as the region of all simultaneously achievable rates and equivocation-rates. In [5], the secrecy capacity region was established for the general case where the eavesdropper's channel is not necessarily a degraded version of the main receiver's channel. In particular, it was shown that to achieve the secrecy capacity region of the single user wiretap channel, channel prefixing may be necessary. In channel prefixing, an auxiliary random variable serves as the input of an artificially created prefix channel, whose output is used as the input to the original wiretap channel. In [6], the authors showed that, through plain Gaussian signaling alone, i.e., without channel prefixing, one can achieve the secrecy capacity of the Gaussian wiretap channel.

The multiple access wiretap channel (MAC-WT) was introduced in [7]. In MAC-WT, multiple users wish to have secure communication with a single receiver, in the presence of a passive eavesdropper. References [7] and [8] focus on the Gaussian MAC-WT, and provide achievable schemes based on Gaussian signaling. Reference [8] goes further than plain Gaussian signaling and introduces a technique (on top of Gaussian signaling) that uses the power of a non-transmitting node in jamming the eavesdropper. This technique is called *cooperative jamming*. Cooperative jamming is indeed a channel prefixing technique where specific choices are made for the auxiliary random variables [9]. In addition, cooperative jamming is the first significant application of channel prefixing in a multi-user Gaussian wiretap channel that improves over plain Gaussian signaling. More recently, reference [10] showed that for a certain class of Gaussian MAC-WT, one can achieve through Gaussian signaling a secrecy rate region that is within 0.5 bits of the secrecy capacity region. Consequently, there has been some expectation that secrecy capacity may be obtained for Gaussian MAC-WT through i.i.d. Gaussian signaling, potentially with Gaussian channel prefixing.

However, a notable shortcoming of these Gaussian signaling based achievable schemes is that rates obtained using them do not scale with the signal-to-noise ratio (SNR). In other words, the total number of degrees of freedom (DoF) for the MAC-WT achieved using these schemes is zero. This observation led to the belief that these schemes, and hence Gaussian signaling (with or without channel prefixing), may be sub-optimal. This belief is made certain as a direct consequence of the results on the secure DoF of Gaussian interference networks that were obtained in several papers, e.g., in [11], [12], [13], [14], and [15]. In particular, in each of [11] and [12], it was shown that positive secure DoF is achievable for a class of vector Gaussian interference channels (i.e., time-varying channels where channel state information is known non-causally) which in turn implies that positive secure DoF is achievable for the vector Gaussian MAC-WT. In [13] and [14], it was shown that through structured coding (e.g., lattice coding), it is possible to achieve positive DoF for a class of scalar (i.e., non-time-varying) Gaussian channels with interference that contains the Gaussian MAC-WT. More recently, in [15], an achievable secrecy rate region for the K-user Gaussian MAC-WT was obtained by incorporating a new alignment technique known as real interference alignment. This technique performs on a single real line and exploits the properties of real numbers to align interference in time-invariant channels.

Fading Gaussian MAC-WT was first considered in [16] where the Gaussian signaling and cooperative jamming schemes which were originally proposed in [7] and [8] are extended to the fading MAC-WT. Using these schemes, [16] gave achievable ergodic sum secrecy rates for the fading MAC-WT. Similar to the non-fading setting, these achievable ergodic secrecy rates do not scale with the average SNRs. In this paper, we propose two new achievable schemes for the fading Gaussian MAC-WT. Our first achievable scheme, the *scaling based alignment* (SBA) scheme, is based on code repetition with proper scaling of transmitted signals. In particular, transmitters repeat their symbols in two *consecutive* symbol instants. Transmitters further scale their transmit signals with the goal of creating a full-rank channel matrix at the main receiver and a unit-rank channel matrix at the eavesdropper, in every two consecutive time instants. These coordinated actions create a two-dimensional space for the signal received by the legitimate receiver, while sustaining the interference in a single-dimensional space at the eavesdropper. In other words, code repetition with proper scaling of the transmit signals at each transmitter *aligns* the received signals at the eavesdropper perfectly making it difficult for the eavesdropper to decode both messages. Consequently, we obtain a new achievable secrecy rate region for the two-user fading MAC-WT.

In another recent work [17], it was shown that in a fading interference channel, by code repetition over *properly chosen* time instants, one can perfectly cancel interference at each receiver so that the resulting individual rates scale as $\frac{1}{2}\log(\text{SNR})$. Thus, the rate reduction by a factor of $\frac{1}{2}$ comes with the benefit of perfect interference cancellation. In this paper, we extend the ergodic interference alignment concept to a secrecy context and we propose another achievable scheme which we call *ergodic secret alignment* (ESA). In the SBA scheme, code repetition is done over two consecutive time instants, while in the ESA scheme, we carefully choose the time instants over which we do code repetition such that the received signals are aligned favorably at the legitimate receiver while they are aligned unfavorably at the eavesdropper. In particular, given some time instant with the vector of the main receiver channel coefficients and the vector of the eavesdropper channel coefficients given by $\mathbf{h} = [h_1\ h_2]^T$ and $\mathbf{g} = [g_1\ g_2]^T$, respectively, if X_1 and X_2 are the symbols transmitted in this time instant by users 1 and 2, respectively, our objective, roughly speaking, is to determine the channel gains we should wait for to transmit X_1 and X_2 again. In this paper, we show that, in order to maximize achievable secrecy rates, we should wait for a time instant in which the main receiver channel coefficients are $[h_1 \ \ -h_2]^T$ and the eavesdropper channel coefficients are $[g_1 \ g_2]^T$. Consequently, we obtain another achievable secrecy rate region for the two-user fading MAC-WT.

For both proposed schemes, we show that the resulting secrecy rates scale with SNR. Specifically, the achievable secrecy sum rate scales as $1/2 \log(\text{SNR})$. Moreover, we show that the secrecy rates achieved through i.i.d. Gaussian signaling with cooperative jamming in fading MAC-WT do not scale with SNR. The significance of these results is that, they show that indeed neither plain i.i.d. Gaussian signaling nor i.i.d. Gaussian signaling with cooperative jamming is optimal for the fading MAC-WT, and that, for high SNRs, one can achieve higher secrecy rates by aligning interference perfectly in the eavesdropper MAC while reducing, or cancelling, interference at the main receiver MAC using some coordinated actions at both transmitters that involve code repetition, i.e., a form of time-correlated (non i.i.d.) signaling.

In fact, the achievable rate region using the second scheme, the ESA scheme, involves two significant improvements over the one achieved by the SBA scheme when the channel coefficients are circularly symmetric complex Gaussian random variables. First, the expressions for achievable rates by the SBA scheme involve products of the squared magnitudes of the channel coefficients. The squared magnitudes of the channel coefficients are exponential random variables and hence multiplying them will intuitively make the small values of their product occur with higher probability and the large values occur with lower probability. This in effect reduces the achievable rates by the SBA scheme. On the other hand, the achievable secrecy rates by the ESA scheme do not have this drawback. In other words, by code repetition, the SBA scheme creates two (not perfectly) correlated MAC channels to the main receiver and two perfectly correlated MAC channels to the eavesdropper, while the ESA scheme creates an orthogonal MAC channel to the main receiver and two perfectly correlated MAC channels to the eavesdropper. This fact leads to higher achievable secrecy rates by the ESA scheme. The second improvement of the ESA scheme with respect to the SBA scheme is that the average power constraints associated with the ESA scheme do not involve any channel coefficients whereas those associated with the SBA scheme involve the gains of the eavesdropper channel which in turn result in inefficient use of transmit powers.

In addition, we introduce an improved version of our second scheme in which we use cooperative jamming on top of the ESA scheme to achieve higher secrecy rates. Moreover, since the rate expressions achieved by the ESA scheme (with and without cooperative jamming) and their associated average power constraints are simpler than their counterparts in the SBA scheme, we derive the necessary conditions on the optimal power allocations that maximize the sum secrecy rate achieved by the ESA scheme when used alone and when used together with cooperative jamming. Since the achievable secrecy sum rate, in general, is not a concave function in the power allocation policy, the solution of such optimization problem may not be unique. Hence, we obtain a power allocation policy that satisfies the necessary (but not necessarily sufficient) KKT conditions of optimality.

Finally, we provide numerical examples that illustrate the scaling of the sum rates achieved by the proposed schemes with SNR and the saturation of the secrecy sum rate achieved by the i.i.d. Gaussian signaling scheme with cooperative jamming. We also give numerical examples for the secrecy sum rates achieved by the ESA scheme with and without cooperative jamming when power control is used.

2 System Model

We consider the two-user fading multiple access channel with an external eavesdropper. Transmitter k chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, ..., 2^{2nR_k}\}$, $k = 1, 2$. Every transmitter encodes its message into a codeword of length $2n$ symbols. The channel output at the intended receiver and the eavesdropper are given by

$$Y = h_1 X_1 + h_2 X_2 + N \tag{1}$$

$$Z = g_1 X_1 + g_2 X_2 + N' \tag{2}$$

where, for $k = 1, 2$, X_k is the input signal at transmitter k, h_k is the channel coefficient between transmitter k and the intended receiver, g_k is the channel coefficient between transmitter k and the eavesdropper. We assume a fast fading scenario where the channel coefficients randomly vary from one symbol to another in i.i.d. fashion. Also, we assume the independence of all channel coefficients h_1, h_2, g_1, and g_2. Each of the channel coefficients is a circularly symmetric complex Gaussian random variable with zero-mean. The variances of h_k and g_k are $\sigma^2_{h_k}$ and $\sigma^2_{g_k}$, respectively. Hence, $|h_k|^2$ and $|g_k|^2$ are exponentially distributed random variables with mean $\sigma^2_{h_k}$ and $\sigma^2_{g_k}$, respectively. Moreover, we assume that all the channel coefficients are known to all the nodes in a causal fashion. In (1)-(2), N and N' are the independent Gaussian noises at the intended receiver and the eavesdropper, respectively, and are i.i.d. (in time) circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. Moreover, we have the usual average power constraints

$$E[|X_k|^2] \leq \bar{P}_k, \quad k = 1, 2. \tag{3}$$

3 Previously Known Results

Here we summarize previously known results that are relevant to our development. For the general discrete-time memoryless MAC-WT, the best known achievable secrecy rate region [7], [8], [9] is given by the convex hull of all rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(V_1; Y|V_2) - I(V_1; Z) \tag{4}$$

$$R_2 \leq I(V_2; Y|V_1) - I(V_2; Z) \tag{5}$$

$$R_1 + R_2 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \tag{6}$$

where the distribution $p(x_1, x_2, v_1, v_2, y, z)$ factors as $p(v_1)p(x_1|v_1)p(v_2)p(x_2|v_2)p(y, z|x_1, x_2)$.

Known secrecy rate regions for the Gaussian MAC-WT can be obtained from these expressions by appropriate selections for the involved random variables. For instance, the Gaussian signaling based achievable rates proposed in [7] are obtained by choosing $X_1 = V_1$ and $X_2 = V_2$, i.e., no channel prefixing, and by choosing X_1 and X_2 to be Gaussian with full power. On the other hand, cooperative jamming based achievable rates proposed in [8] are obtained by choosing $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then by choosing V_1, V_2, T_1, T_2 to be independent Gaussian random variables [9]. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the power constraints of users 1 and 2, respectively. These selections yield the following achievable rate region for the Gaussian MAC-WT [8]

$$R_1 \leq \log\left(1 + \frac{|h_1|^2 P_1}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1 + |g_1|^2 Q_1 + |g_2|^2 (P_2 + Q_2)}\right) \tag{7}$$

$$R_2 \leq \log\left(1 + \frac{|h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1 + |g_1|^2 (P_1 + Q_1) + |g_2|^2 Q_2}\right) \tag{8}$$

$$R_1 + R_2 \leq \log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 Q_2}\right) \tag{9}$$

where the powers of the signals must satisfy

$$P_k + Q_k \leq \bar{P}_k, \quad k = 1, 2 \tag{10}$$

where P_k and Q_k are the transmission and jamming powers, respectively, of user k.

The ergodic secrecy rate region achieved by Gaussian signaling and cooperative jamming for the fading MAC-WT can be expressed similarly by simply including expectations over fading channel states [16]

$$R_1 \leq E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + \frac{|h_1|^2 P_1}{1+|h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1+|g_1|^2 Q_1 + |g_2|^2 (P_2+Q_2)}\right)\right\} \tag{11}$$

$$R_2 \leq E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + \frac{|h_2|^2 P_2}{1+|h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1+|g_1|^2 (P_1+Q_1) + |g_2|^2 Q_2}\right)\right\} \tag{12}$$

$$R_1 + R_2 \leq E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1+|h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1+|g_1|^2 Q_1 + |g_2|^2 Q_2}\right)\right\} \tag{13}$$

where $\mathbf{h} = [h_1 \ h_2]^T$, $\mathbf{g} = [g_1 \ g_2]^T$, and the instantaneous powers P_k and Q_k, which are both functions of $\mathbf{h}$ and $\mathbf{g}$, satisfy

$$E\left[P_k + Q_k\right] \leq \bar{P}_k, \ \ k = 1, 2 \tag{14}$$

4 Scaling Based Alignment (SBA)

In this section, we introduce a new achievable scheme for the fading MAC-WT. Our achievable scheme is based on code repetition with proper scaling of the signals transmitted by each transmitter. This is done as follows. For the channel described in (1)-(2), we use a repetition code such that each transmitter repeats its channel input symbol twice over two *consecutive* time instants. Due to code repetition, we may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for the *odd* time instants and the other for the *even* time instants. Consequently, we may describe the main receiver MAC channel by the following pair of equations

$$Y_o = h_{1o} X_1 + h_{2o} X_2 + N_o \tag{15}$$

$$Y_e = h_{1e} X_1 + h_{2e} X_2 + N_e \tag{16}$$

where, for $k = 1, 2$, h_{ko}, h_{ke} are the coefficients of the kth main receiver channel in odd and even time instants, Y_o, Y_e and N_o, N_e are the received signal and the noise at the main receiver in odd and even time instants. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations

$$Z_o = g_{1o} X_1 + g_{2o} X_2 + N'_o \tag{17}$$

$$Z_e = g_{1e} X_1 + g_{2e} X_2 + N'_e \tag{18}$$

where, for $k = 1, 2$, g_{ko}, g_{ke} are the coefficients of the kth eavesdropper channel in odd and even time instants, Z_o, Z_e and N_o, N_e are the received signal and the noise at the eavesdropper in odd and even time instants.

Since all the channel gains are known to all nodes in a causal fashion, the two transmitters use this knowledge as follows. In every symbol instant, each transmitter scales its transmit signal with the gain of the other transmitter's channel to the eavesdropper. That is, in every symbol duration, the first user multiplies its channel input with g_2, the channel gain of the second user to the eavesdropper, and the second user multiplies its channel input with g_1, the channel gain of the first user to the eavesdropper. Hence the main receiver MAC can be described as

$$Y_o = h_{1o}g_{2o}X_1 + h_{2o}g_{1o}X_2 + N_o \tag{19}$$

$$Y_e = h_{1e}g_{2e}X_1 + h_{2e}g_{1e}X_2 + N_e \tag{20}$$

and the eavesdropper MAC can be described as

$$Z_o = g_{1o}g_{2o}X_1 + g_{1o}g_{2o}X_2 + N'_o \tag{21}$$

$$Z_e = g_{1e}g_{2e}X_1 + g_{2e}g_{2e}X_2 + N'_e \tag{22}$$

It is clear from (19)-(20) that the space of the received signal (without noise, i.e., high SNR) of the main receiver over the two consecutive time instants is two-dimensional almost surely. In other words, the channel matrix of the main receiver vector MAC is full-rank almost surely. This is due to the fact that the channel coefficients are drawn from continuous bounded distributions. On the other hand, it is clear from (21)-(22) that the channel matrix of the eavesdropper vector MAC is unit-rank. That is, the two ingredients of our scheme, i.e., code repetition and signal scaling, let the interfering signals at the main receiver live in a two-dimensional space, while they *align* the interfering signals at the eavesdropper in a one-dimensional space. As we will show in the Section 6, these properties play a central role in achieving secrecy rates that scale with SNR. Finally, we note that, due to signal scaling at the transmitters, the average power constraints become

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \leq \bar{P}_1 \tag{23}$$

$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \leq \bar{P}_2 \tag{24}$$

where P_1 and P_2, which are functions of the channel gains, are the instantaneous powers of users 1 and 2, respectively.

Now, we evaluate the secrecy rate region achievable by our *scaling based alignment* (SBA) scheme. Given the vector channels (19)-(20) and (21)-(22), the following secrecy rates are achievable [7], [8], [9],

$$R_1 \le \frac{1}{2}\left[I(X_1; Y_o, Y_e|X_2, \mathbf{h}, \mathbf{g}) - I(X_1; Z_o, Z_e|\mathbf{h}, \mathbf{g})\right] \tag{25}$$

$$R_2 \le \frac{1}{2}\left[I(X_2; Y_o, Y_e|X_1, \mathbf{h}, \mathbf{g}) - I(X_2; Z_o, Z_e|\mathbf{h}, \mathbf{g})\right] \tag{26}$$

$$R_1 + R_2 \le \frac{1}{2}\left[I(X_1, X_2; Y_o, Y_e|\mathbf{h}, \mathbf{g}) - I(X_1, X_2; Z_o, Z_e|\mathbf{h}, \mathbf{g})\right] \tag{27}$$

These expressions for achievable rates follow from (4)-(6) by treating channel states as outputs at the receivers, and noting the independence of channel inputs and channel states. We note that the factor of 1/2 on the right hand sides of (25)-(27) is due to repetition coding. Now, by computing (25)-(27) with Gaussian signals, we obtain the secrecy rate region given in the following theorem.

Theorem 1 *For the two-user fading MAC-WT, the rate region given by all rate pairs (R_1, R_2) satisfying the following constraints is achievable with perfect secrecy*

$$R_1 \le \frac{1}{2}E_{\boldsymbol{h},\boldsymbol{g}}\left\{\log\left(1 + (|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2)P_1\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}\right)\right\} \tag{28}$$

$$R_2 \le \frac{1}{2}E_{\boldsymbol{h},\boldsymbol{g}}\left\{\log\left(1 + (|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2)P_2\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}\right)\right\} \tag{29}$$

$$\begin{aligned} R_1 + R_2 \le \frac{1}{2}E_{\boldsymbol{h},\boldsymbol{g}}\Bigg\{ &\log\Bigg(1 + \left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right)P_1 + \left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right)P_2 \\ &\qquad + |h_{1e}h_{2o}g_{1o}g_{2e} - h_{1o}h_{2e}g_{1e}g_{2o}|^2 P_1 P_2\Bigg) \\ &- \log\left(1 + \left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)(P_1 + P_2)\right)\Bigg\} \end{aligned} \tag{30}$$

where $\boldsymbol{h} = [h_{1o}\ h_{1e}\ h_{2o}\ h_{2e}]^T$, $\boldsymbol{g} = [g_{1o}\ g_{1e}\ g_{2o}\ g_{2e}]^T$, and P_1, P_2, which are functions of $\boldsymbol{h}_o = [h_{1o}\ h_{2o}]^T$ and $\boldsymbol{g}_o = [g_{1o}\ g_{2o}]^T$, are the power allocation policies of users 1 and 2, respectively, that satisfy

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right)P_1\right] \le \bar{P}_1 \tag{31}$$

$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right)P_2\right] \le \bar{P}_2 \tag{32}$$

where $\bar{P}_1$ and $\bar{P}_2$ are the average power constraints.

5 Ergodic Secret Alignment (ESA)

After we have devised the scaling based alignment scheme, the ergodic interference alignment scheme of Nazer *et. al.* [17] inspired us to propose an improved achievable scheme. In this section, we discuss this scheme which we call *ergodic secret alignment* (ESA). The new ingredient in this scheme is to perform repetition coding at two *carefully chosen* time instances as opposed to two *consecutive* time instances as we have done in Section 4.

For the MAC-WT described by (1)-(2), we use a repetition code in a way similar to the one in [17]. Indeed, we repeat each code symbol in the time instant that holds certain channel conditions relative to the those conditions in the time instant where this code symbol is first transmitted. Namely, given a time instant with the main receiver channel state vector $\mathbf{h} = [h_1 \ h_2]^T$ and the eavesdropper channel state vector $\mathbf{g} = [g_1 \ g_2]^T$, where the symbols X_1 and X_2 are first transmitted by the two transmitters, we will solve for the channel states $\tilde{\mathbf{h}} = [\tilde{h}_1 \ \tilde{h}_2]^T$ and $\tilde{\mathbf{g}} = [\tilde{g}_1 \ \tilde{g}_2]^T$, where these symbols should be repeated again, such that the resulting secrecy rates achieved by Gaussian signaling are maximized.

Due to code repetition, we may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for each one of the two time instants over which the same code symbols X_1 and X_2 are transmitted. Consequently, we may describe the main receiver MAC channel by the following pair of equations

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{33}$$

$$Y_2 = \tilde{h}_1 X_1 + \tilde{h}_2 X_2 + N_2 \tag{34}$$

where Y_1, Y_2 and N_1, N_2 are the received symbols and the noise at the main receiver in the two time instants of code repetition. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations

$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{35}$$

$$Z_2 = \tilde{g}_1 X_1 + \tilde{g}_2 X_2 + N_2' \tag{36}$$

where Z_1, Z_2 and N_1', N_2' are the received symbols and the noise at the eavesdropper in the two time instants of code repetition.

In the next theorem, we give another achievable secrecy rate region for the two-user fading MAC-WT. The achievable region is obtained using (25)-(27) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2), respectively, and evaluating these expressions with Gaussian signals, and by choosing optimal $\tilde{\mathbf{h}} = (\tilde{h}_1, \tilde{h}_2)$ and $\tilde{\mathbf{g}} = (\tilde{g}_1, \tilde{g}_2)$ to maximize the achievable rates. In particular, we choose the repetition instants, i.e., $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$, in such a way that the parallel MAC to the main receiver is the most favorable from the main transmitter-receiver pair's point of view, and the parallel MAC to the eavesdropper is the least favorable from the eavesdropper's point of view. As we will show shortly as a result of Theorem 2, this optimal selection will yield an *orthogonal* MAC to the main receiver and a *scalar* MAC to the eavesdropper. In writing the achievable rate expressions, we will again account for code repetition by multiplying achievable rates by a factor of 1/2.

Theorem 2 *For the two-user fading MAC-WT, the rate region given by all rate pairs (R_1, R_2) satisfying the following constraints is achievable with perfect secrecy*

$$R_1 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1 + 2|g_2|^2 P_2}\right) \right\} \tag{37}$$

$$R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1 + 2|g_1|^2 P_1}\right) \right\} \tag{38}$$

$$R_1 + R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \right\} \tag{39}$$

where P_1 and P_2 are the power allocation policies of users 1 and 2, respectively, and are both functions of $\boldsymbol{h}$ and $\boldsymbol{g}$ in general. In addition, they satisfy the average power constraints

$$E[P_1] \leq \bar{P}_1 \tag{40}$$

$$E[P_2] \leq \bar{P}_2 \tag{41}$$

Proof: First, consider the two vector MACs given by (33)-(36). Observe that as in [17], $\tilde{\mathbf{h}}$ must be chosen such that it has the same distribution as $\mathbf{h}$ and $\tilde{\mathbf{g}}$ must be chosen such that it has the same distribution as $\mathbf{g}$. Since $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_h)$ and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_g)$ where $\mathbf{B}_h = \text{diag}(\sigma_{h_1}^2, \sigma_{h_2}^2)$ and $\mathbf{B}_g = \text{diag}(\sigma_{g_1}^2, \sigma_{g_2}^2)$, then $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ must be in the form $\tilde{\mathbf{h}} = \mathbf{U}\mathbf{h}$ and $\tilde{\mathbf{g}} = \mathbf{V}\mathbf{g}$ where the unitary matrices $\mathbf{U}$ and $\mathbf{V}$ must further be of the form: $\mathbf{U} = \text{diag}(\exp(j\theta_1), \exp(j\theta_2))$ and $\mathbf{V} = \text{diag}(\exp(j\omega_1), \exp(j\omega_2))$ for some $\theta_1, \theta_2, \omega_1, \omega_2 \in [0, 2\pi)$. Then, it follows that (33)-(36) can be written as

$$\begin{aligned} Y_1 &= h_1 X_1 + h_2 X_2 + N_1 & (42)\\ Y_2 &= h_1 e^{j\theta_1} X_1 + h_2 e^{j\theta_2} X_2 + N_2 & (43)\\ Z_1 &= g_1 X_1 + g_2 X_2 + N_1' & (44)\\ Z_2 &= g_1 e^{j\omega_1} X_1 + g_2 e^{j\omega_2} X_2 + N_2' & (45) \end{aligned}$$

Using (25)-(27) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2), respectively, and computing these achievable rates with Gaussian signals, we get

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_1|^2P_1\right) - \log\left(1+\frac{2|g_1|^2P_1+2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2}{1+2|g_2|^2P_2}\right)\right\} \tag{46}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_2|^2P_2\right) - \log\left(1+\frac{2|g_2|^2P_2+2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2}{1+2|g_1|^2P_1}\right)\right\} \tag{47}$$

$$\begin{aligned} R_1+R_2 \leq& \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log(1+2|h_1|^2P_1+2|h_2|^2P_2+2(1-\cos(\theta))|h_1|^2|h_2|^2P_1P_2) \\ &- \log(1+2|g_1|^2P_1+2|g_2|^2P_2+2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2)\Big\} \end{aligned} \tag{48}$$

where $\theta = \theta_2 - \theta_1$ and $\omega = \omega_2 - \omega_1$.

Hence, the largest achievable secrecy rate region (46)-(48) is attained by choosing $\theta = \pi$ and $\omega = 0$. This can be achieved by choosing $\theta_1 = 0$ and $\theta_2 = \pi$ and by choosing $\omega_1 = \omega_2 = 0$. Consequently, we have $\tilde{\mathbf{h}} = [h_1 \ - h_2]^T$ and $\tilde{\mathbf{g}} = [g_1 \ g_2]^T$. By substituting these values of θ and ω in (46)-(48), we obtain the region given by (37)-(39). ■

Therefore, when using the ergodic secret alignment technique, the best choice for $\tilde{h}_1$ and $\tilde{h}_2$ is such that $\tilde{\mathbf{h}}$ is orthogonal to $\mathbf{h}$ and that $\|\tilde{\mathbf{h}}\| = \|\mathbf{h}\|$, and the best choice for $\tilde{g}_1$ and $\tilde{g}_2$ is such that $\tilde{\mathbf{g}}$ and $\mathbf{g}$ are linearly dependent and that $\|\tilde{\mathbf{g}}\| = \|\mathbf{g}\|$, i.e., $\tilde{\mathbf{g}} = \mathbf{g}$. This choice makes the vector MAC between the two transmitters and the main receiver equivalent to an orthogonal MAC, i.e., two independent single-user fading channels, one from each transmitter to the main receiver. This equivalent main receiver MAC channel can be expressed as

$$\bar{Y}_1 = 2h_1X_1 + \bar{N}_1 \tag{49}$$

$$\bar{Y}_2 = 2h_2X_2 + \bar{N}_2 \tag{50}$$

where $\bar{Y}_1 = Y_1 + Y_2$, $\bar{Y}_2 = Y_1 - Y_2$, $\bar{N}_1 = N_1 + N_2$, and $\bar{N}_2 = N_1 - N_2$. Note that $\bar{N}_1$ and $\bar{N}_2$ are independent. On the other hand, this choice makes the vector MAC between the two transmitters and the eavesdropper equivalent to a single scalar MAC. This equivalent eavesdropper MAC channel can be expressed as

$$\bar{Z}_1 = 2g_1X_1 + 2g_2X_2 + \bar{N}_1' \tag{51}$$

$$\bar{Z}_2 = \bar{N}_2' \tag{52}$$

where $\bar{Z}_1 = Z_1 + Z_2$, $\bar{Z}_2 = Z_1 - Z_2$, $\bar{N}_1' = N_1' + N_2'$, and $\bar{N}_2' = N_1' - N_2'$. Note again that $\bar{N}_1$ and $\bar{N}_2$ are independent. Note that, here, the second component of the eavesdropper's vector MAC is useless for her (i.e., leaks no further information than the first component) as it contains only noise. This selection of the repetition channel state yields a most favorable setting for the main receiver, and a least favorable setting for the eavesdropper.

6 Degrees of Freedom

In this section, we show that the secrecy sum rates achieved by our schemes scale with SNR as $1/2\log(\text{SNR})$ and that the secrecy sum rate achieved by the cooperative jamming scheme given in [16] does not scale with SNR. What we give here are rigorous proofs for intuitive results. Since by looking at (30) and (39), one can note that, if we assume that $\bar{P}_1 = \bar{P}_2 = P$, then if we take $P_1 = P_2 = P$, as P becomes large, roughly speaking, in (30) the first term inside the expectation grows as $\log(P^2)$ while the second term grows as $\log(P)$ and hence the overall expression grows as $1/2\log(P)$; and similarly, in (39), all three terms inside the expectation grow as $\log(P)$ and hence the overall expression grows as $1/2\log(P)$. In the same way, by considering the secrecy sum rate achieved by the cooperative jamming scheme given in (13), then by referring to the power allocation policies given in [16], one can also roughly say that for all channel states, as the available average power goes to infinity, the overall expression converges to a constant.

For simplicity, we assume symmetric average power constraints for all schemes, i.e., we set $\bar{P}_1 = \bar{P}_2 = P$ in (31)-(32), (40)-(41), and (14). We also assume that all channel gains are drawn from continuous bounded distributions and that all channel gains have finite variances. Let R_s be the achievable secrecy sum rate, then the total number of achievable secure DoF, η, is defined as

$$\eta \triangleq \lim_{P\rightarrow\infty} \frac{R_s}{\log(P)} \tag{53}$$

We start by the DoF analysis of our proposed schemes, i.e., the SBA scheme and the ESA scheme, where we show that the sum secrecy rates obtained by these schemes achieve 1/2 secure DoF, then we provide a rigorous proof for the fact that the scheme of [16] which is based on i.i.d. Gaussian signaling with cooperative jamming achieves a secrecy sum rate that does not scale with SNR, i.e., achieves zero secure DoF.

6.1 Secure DoF with the SBA Scheme

We make the following choices for the power allocation policies P_1 and P_2 of the SBA scheme. We set $P_1 = \frac{1}{2\sigma^2_{g_2}}P$, $P_2 = \frac{1}{2\sigma^2_{g_1}}P$. It can be verified that these choices satisfy the power constraints (31)-(32). Denoting the expression inside the expectation in (30) by $f_P(\mathbf{h},\mathbf{g})$, the secrecy sum rate achieved using the SBA scheme can be written as

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{f_P(\mathbf{h},\mathbf{g})\right\} \tag{54}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2}\lim_{P\rightarrow\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] \tag{55}$$

Now, we show that, for the two-user fading MAC-WT, a total number of secure DoF $\eta = 1/2$ is achievable with the SBA scheme. Towards this end, it suffices to show that the order of the limit and the expectation in (55) can be reversed. To do this, we make use of Lebesgue dominated convergence theorem. Now, we note that for large enough P, $\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}$ is upper bounded by $\psi(\mathbf{h},\mathbf{g})$ where

$$\begin{aligned}\psi(\mathbf{h},\mathbf{g}) =& 4+2\left(\log\left(1+\frac{1}{\sigma_{g_1}^2}\right)+\log\left(1+\frac{1}{\sigma_{g_2}^2}\right)\right)+\log\left(1+\frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right)\\ &+3\left(\sum_{k=1}^{2}\log(1+|h_{ko}|^2)+\sum_{k=1}^{2}\log(1+|h_{ke}|^2)\right)\\ &+4\left(\sum_{k=1}^{2}\log(1+|g_{ko}|^2)+\sum_{k=1}^{2}\log(1+|g_{ke}|^2)\right) \qquad (56)\end{aligned}$$

Hence, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}\left[\psi(\mathbf{h},\mathbf{g})\right] < \infty \qquad (57)$$

Thus, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = E_{\mathbf{h},\mathbf{g}}\left[\lim_{P\to\infty}\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = 1 \qquad (58)$$

Hence, from (55), we have $\eta = 1/2$.

6.2 Secure DoF with the ESA Scheme

We show that the ESA scheme achieves $\eta = 1/2$ secure DoF in the two-user fading MAC-WT. Here, we also use a constant power allocation policy for the ESA scheme where we set $P_1 = P_2 = P$ for all channel states. Clearly, this constant policy satisfies the average power constraints (40)-(41). Denoting the expression inside the expectation in (39) by $\tilde{f}_P(\mathbf{h},\mathbf{g})$, the achievable secrecy sum rate, R_s is given by

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{\tilde{f}_P(\mathbf{h},\mathbf{g})\right\} \qquad (59)$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2}\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] \qquad (60)$$

We note that for large enough P, $\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \leq \tilde{\psi}(\mathbf{h},\mathbf{g})$ where

$$\tilde{\psi}(\mathbf{h},\mathbf{g}) = 6 + \log\left(1+2|h_1|^2\right) + \log\left(1+2|h_2|^2\right) + \log\left(1+2\left(|g_1|^2+|g_2|^2\right)\right) \tag{61}$$

Again, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}\left[\tilde{\psi}(\mathbf{h},\mathbf{g})\right] < \infty \tag{62}$$

Then, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = E_{\mathbf{h},\mathbf{g}}\left[\lim_{P\to\infty}\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = 1 \tag{63}$$

Hence, from (60), we have $\eta = 1/2$.

6.3 Secure DoF with i.i.d. Gaussian Signaling with CJ

We consider the secrecy sum rate achieved by Gaussian signaling with cooperative jamming (CJ) [16] in the fading MAC-WT and show that this achievable rate does not scale with SNR. We start with the secrecy sum rate given by the right hand side of (13). According to the optimal power allocation policy described in [16], for $k = 1, 2$, we cannot have $P_k > 0$ and $Q_k > 0$ simultaneously. Moreover, no transmission occurs when $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$. Consequently, according to the relative values of the channel gains $(|h_1|, |h_2|, |g_1|, |g_2|)$, there are three different cases left for the instantaneous secrecy sum rate achieved using the optimum power allocation where we omitted the case where $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$ since no transmission is allowed.

Case 1: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_1$ where $\mathcal{D}_1 = \left\{(\mathbf{h},\mathbf{g}) : |h_1| > |g_1|, |h_2| > |g_2|\right\}$. Consequently, $Q_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$R_s(\mathbf{h},\mathbf{g}) = \log\left(\frac{1+|h_1|^2P_1+|h_2|^2P_2}{1+|g_1|^2P_1+|g_2|^2P_2}\right) \tag{64}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$R_s(\mathbf{h},\mathbf{g}) \leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}+\frac{|h_2|^2}{|g_2|^2}\right) \leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1+\frac{|h_2|^2}{|g_2|^2}\right) \tag{65}$$

Case 2: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_2$ where $\mathcal{D}_2 = \left\{(\mathbf{h},\mathbf{g}) : |h_1| > |g_1|, |h_2| < |g_2|\right\}$. Consequently, $Q_1 = P_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$R_s(\mathbf{h},\mathbf{g}) = \log\left(\frac{1+|h_1|^2P_1+|h_2|^2Q_2}{1+|g_1|^2P_1+|g_2|^2Q_2}\right) + \log\left(\frac{1+|g_2|^2Q_2}{1+|h_2|^2Q_2}\right) \tag{66}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1 + \log\left(1 + \frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1 + \frac{|g_2|^2}{|h_2|^2}\right) \tag{67}$$

Case 3: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_3$ where $\mathcal{D}_3 = \big\{(\mathbf{h},\mathbf{g}) : |h_1| < |g_1|, |h_2| > |g_2|\big\}$. Consequently, $P_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$R_s(\mathbf{h},\mathbf{g}) = \log\left(\frac{1 + |h_1|^2 Q_1 + |h_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 P_2}\right) + \log\left(\frac{1 + |g_1|^2 Q_1}{1 + |h_1|^2 Q_1}\right) \tag{68}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1 + \log\left(1 + \frac{|h_2|^2}{|g_2|^2}\right) + \log\left(1 + \frac{|g_1|^2}{|h_1|^2}\right) \tag{69}$$

Now, since the instantaneous sum rate is zero outside $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$, then from (65), (67), and (69), the ergodic secrecy sum rate, R_s, can be upper bounded as follows

$$\begin{aligned} R_s \leq & \int_{\mathcal{D}_1} \left(\log\left(1 + \frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1 + \frac{|h_2|^2}{|g_2|^2}\right)\right) d\mathbf{F} \\ & + \int_{\mathcal{D}_2} \left(1 + \log\left(1 + \frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1 + \frac{|g_2|^2}{|h_2|^2}\right)\right) d\mathbf{F} \\ & + \int_{\mathcal{D}_3} \left(1 + \log\left(1 + \frac{|h_2|^2}{|g_2|^2}\right) + \log\left(1 + \frac{|g_1|^2}{|h_1|^2}\right)\right) d\mathbf{F} \end{aligned} \tag{70}$$

where

$$d\mathbf{F} = \prod_{k=1}^{2} f(|h_k|^2) f(|g_k|^2) d|h_k|^2 d|g_k|^2 \tag{71}$$

where, for $k = 1, 2$, $f(|h_k|^2)$ and $f(|g_k|^2)$ are the density functions of $|h_k|^2$ and $|g_k|^2$, respectively. Now, since $E[|h_k|^2] < \infty$, $E[|g_k|^2] < \infty$ for $k = 1, 2$, $|\int_0^1 \log(x)dx| = \log(e) < \infty$, $|\int_0^1 \log(1+x)dx| = 2 - \log(e) < \infty$, and $f(|h_k|^2), f(|g_k|^2)$ are continuous and bounded for $k = 1, 2$, it follows that each of the three integrals in the above expression is finite. Hence, we have $R_s < \infty$, and that R_s is bounded from above by a constant. Thus, from definition (53) of the achievable secure DoF, η, we have

$$\eta = \lim_{P\to\infty} \frac{R_s}{\log(P)} = 0 \tag{72}$$

7 ESA Scheme with Cooperative Jamming

The result given in Theorem 2 can be strengthened by adding the technique of cooperative jamming to the ESA scheme of Section 5. We refer to the resulting scheme as ESA/CJ. This is done through Gaussian channel prefixing as discussed in Section 3. In particular, we choose the channel inputs in (33)-(36) to be $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then choose V_1, V_2, T_1, T_2 to be independent Gaussian random variables. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the average power constraints of users 1 and 2, respectively. These selections when made in the ESA scheme yield the following achievable rate region which, through appropriate power control strategy (see Section 9), can be made strictly larger than the region given in Theorem 2,

$$R_1 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{ \log\left(1+\frac{2|h_1|^2P_1}{1+2|h_1|^2Q_1}\right) - \log\left(1+\frac{2|g_1|^2P_1}{1+2|g_1|^2Q_1+2|g_2|^2(P_2+Q_2)}\right)\right\} \tag{73}$$

$$R_2 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{ \log\left(1+\frac{2|h_2|^2P_2}{1+2|h_2|^2Q_2}\right) - \log\left(1+\frac{2|g_2|^2P_2}{1+2|g_1|^2(P_1+Q_1)+2|g_2|^2Q_2}\right)\right\} \tag{74}$$

$$\begin{aligned} R_1+R_2 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Bigg\{ & \log\left(1+\frac{2|h_1|^2P_1}{1+2|h_1|^2Q_1}\right) + \log\left(1+\frac{2|h_2|^2P_2}{1+2|h_2|^2Q_2}\right) \\ & - \log\left(1+\frac{2(|g_1|^2P_1+|g_2|^2P_2)}{1+2(|g_1|^2Q_1+|g_2|^2Q_2)}\right)\Bigg\} \end{aligned} \tag{75}$$

where, for $k = 1, 2$, P_k and Q_k are the transmission and jamming powers, respectively, of user k, and are both functions of $\mathbf{h}$ and $\mathbf{g}$ in general. In addition, they satisfy the average power constraints

$$E[P_k + Q_k] \leq \bar{P}_k,\ k = 1, 2 \tag{76}$$

8 Maximizing Secrecy Sum Rate of the ESA Scheme

In this section, we consider the problem of maximizing the secrecy sum rate achieved by the ESA scheme as a function of the power allocations P_1 and P_2 of users 1 and 2, respectively. For notational convenience, we replace $2|h_k|^2$ and $2|g_k|^2$ in the achievable rates (37)-(39) by h_k and g_k, respectively. Then, we define $\mathbf{h} \triangleq [h_1 \quad h_2]^T$ and $\mathbf{g} \triangleq [g_1 \quad g_2]^T$. The achievable secrecy sum rate is given by

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\{\log(1+h_1P_1) + \log(1+h_2P_2) - \log(1+g_1P_1+g_2P_2)\} \tag{77}$$

We can write the optimization problem as

$$\begin{aligned} \max \quad & E_{\mathbf{h},\mathbf{g}}\{\log(1+h_1P_1)+\log(1+h_2P_2)-\log(1+g_1P_1+g_2P_2)\} && (78) \\ \text{s.t.} \quad & E_{\mathbf{h},\mathbf{g}}\left[P_k(\mathbf{h},\mathbf{g})\right] \leq \bar{P}_k, \quad k=1,2 && (79) \\ & P_k(\mathbf{h},\mathbf{g}) \geq 0, \quad k=1,2, \quad \forall \mathbf{h},\mathbf{g} && (80) \end{aligned}$$

The necessary KKT optimality conditions are

$$\frac{h_1}{1+h_1P_1}-\frac{g_1}{1+g_1P_1+g_2P_2}-(\lambda_1-\mu_1)=0 \tag{81}$$

$$\frac{h_2}{1+h_2P_2}-\frac{g_2}{1+g_1P_1+g_2P_2}-(\lambda_2-\mu_2)=0 \tag{82}$$

It should be noted here that (81)-(82) are only necessary conditions for the optimal power allocations P_1 and P_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave in (P_1,P_2) in general.

For each channel state, we distinguish between three non-zero forms that the solution (P_1,P_2) of (81)-(82) may take. First, if $P_1>0$ and $P_2>0$, then $\mu_1=\mu_2=0$. Hence (P_1,P_2) is the positive common root of the following two quadratic equations

$$h_1(1+g_2P_2)-g_1=\lambda_1(1+h_1P_1)(1+g_1P_1+g_2P_2) \tag{83}$$

$$h_2(1+g_1P_1)-g_2=\lambda_2(1+h_2P_2)(1+g_1P_1+g_2P_2) \tag{84}$$

Since it is hard to find a simple closed-form solution for the above system of equations, we solve this system numerically and obtain the positive common root (P_1,P_2). Secondly, if $P_1>0$ and $P_2=0$, then $\mu_1=0$. Hence, from (81), P_1 is given by

$$P_1=\frac{1}{2}\left(\sqrt{\left(\frac{1}{g_1}-\frac{1}{h_1}\right)^2+\frac{4}{\lambda_1}\left(\frac{1}{g_1}-\frac{1}{h_1}\right)}-\left(\frac{1}{g_1}+\frac{1}{h_1}\right)\right) \tag{85}$$

Thirdly, if $P_1=0$ and $P_2>0$, then $\mu_2=0$. Hence, from (82), P_2 is given by

$$P_2=\frac{1}{2}\left(\sqrt{\left(\frac{1}{g_2}-\frac{1}{h_2}\right)^2+\frac{4}{\lambda_2}\left(\frac{1}{g_2}-\frac{1}{h_2}\right)}-\left(\frac{1}{g_2}+\frac{1}{h_2}\right)\right) \tag{86}$$

From conditions (81)-(82), we can derive the following necessary and sufficient conditions for the positivity of the optimal power allocation policies:

$$P_1>0, \qquad \text{if and only if} \quad h_1-\frac{g_1}{(1+g_2P_2)}>\lambda_1 \tag{87}$$

$$P_2>0, \qquad \text{if and only if} \quad h_2-\frac{g_2}{(1+g_1P_1)}>\lambda_2 \tag{88}$$

Consequently, according to conditions (87)-(88), we can divide the set of all possible channel states into 7 partitions such that in each partition the solution (P_1, P_2) will either have one of the three forms stated above or will be zero. Hence, the power allocation policy (P_1, P_2) that satisfies (81)-(82) and (79)-(80) can be fully described in 7 different cases of the channel gains. The details of such cases are given in Appendix A.

9 Maximizing Secrecy Sum Rate of the ESA/CJ Scheme

In this section, we consider the problem of maximizing the achievable secrecy sum rate as a function in the power allocation policies P_1 and P_2 when cooperative jamming technique is used on top of the ESA scheme. Again, for notational convenience, we replace $2|h_k|^2$ and $2|g_k|^2$ in the achievable rates (73)-(75) by h_k and g_k, respectively. Then, we define $\mathbf{h} \triangleq [h_1 \quad h_2]^T$ and $\mathbf{g} \triangleq [g_1 \quad g_2]^T$. In this case, the optimization problem is described as

$$\begin{aligned} \max \quad & E_{\mathbf{h},\mathbf{g}}\big\{ \log\left(1 + h_1(P_1 + Q_1)\right) + \log\left(1 + h_2(P_2 + Q_2)\right) \\ & \qquad - \log\left(1 + g_1(P_1 + Q_1) + g_2(P_2 + Q_2)\right) + \log\left(1 + g_1 Q_1 + g_2 Q_2\right) \\ & \qquad - \log\left(1 + h_1 Q_1\right) - \log\left(1 + h_2 Q_2\right) \big\} & (89) \\ \text{s.t.} \quad & E_{\mathbf{h},\mathbf{g}}\left[P_k(\mathbf{h},\mathbf{g}) + Q_k(\mathbf{h},\mathbf{g})\right] \leq \bar{P}_k, \quad k = 1, 2 & (90) \\ & P_k(\mathbf{h},\mathbf{g}), Q_k(\mathbf{h},\mathbf{g}) \geq 0, \quad k = 1, 2, \ \forall \mathbf{h}, \mathbf{g} & (91) \end{aligned}$$

We first show that, at any fading state, splitting a user's power into transmission and jamming is suboptimal, i.e., an optimum power allocation policy must not have $P_k > 0$ and $Q_k > 0$ simultaneously. We note that whether we split powers or not does not affect the first three terms of the objective function since we can always convert jamming power of user k into transmission power of the same user and vice versa while keeping the sum $P_k + Q_k$ fixed. Hence, we consider the last three terms of the sum rate. For convenience, we define

$$S = \log\left(1 + g_1 Q_1 + g_2 Q_2\right) - \log\left(1 + h_1 Q_1\right) - \log\left(1 + h_2 Q_2\right) \tag{92}$$

Consider, without loss of generality, the power allocation for user 1. We assume that P_1^*, Q_1^* is the optimum power allocation for user 1. We observe that the sign of

$$\frac{\partial S}{\partial Q_1} = \frac{g_1}{1 + g_1 Q_1 + g_2 Q_2} - \frac{h_1}{1 + h_1 Q_1} \tag{93}$$

does not depend on Q_1. Consider a power allocation $P_1 = P_1^* - \alpha, Q_1 = Q_1^* + \alpha$. Hence, we have $P_1 + Q_1 = P_1^* + Q_1^*$ and the first three terms in the expression of the achievable sum rate do not change. On the other hand, if (93) is positive, any positive α results in an increase in the achievable sum rate and jamming with the same sum power is better. While, if (93) is negative, then any negative α results in an increase in the achievable sum rate and transmitting with the same sum power is better. If (93) is zero, then the sum rate does not depend on Q_1 and we can set it to zero, i.e., use the sum power in transmitting. Therefore, the optimum power allocation will have either $P_k > 0$ or $Q_k > 0$, but not both.

Suppose that P_1, P_2, Q_1, and Q_2 are the optimal power allocations. Then, the necessary KKT conditions satisfy

$$\frac{h_1}{1+h_1(P_1+Q_1)} - \frac{g_1}{1+g_1(P_1+Q_1)+g_2(P_2+Q_2)} - (\lambda_1 - \mu_1) = 0 \tag{94}$$

$$\frac{h_2}{1+h_2(P_2+Q_2)} - \frac{g_2}{1+g_1(P_1+Q_1)+g_2(P_2+Q_2)} - (\lambda_2 - \mu_2) = 0 \tag{95}$$

$$\begin{aligned}&\frac{h_1}{1+h_1(P_1+Q_1)} - \frac{g_1}{1+g_1(P_1+Q_1)+g_2(P_2+Q_2)} + \frac{g_1}{1+g_1Q_1+g_2Q_2}\\ &-\frac{h_1}{1+h_1Q_1} - (\lambda_1 - \nu_1) = 0\end{aligned} \tag{96}$$

$$\begin{aligned}&\frac{h_2}{1+h_2(P_2+Q_2)} - \frac{g_2}{1+g_1(P_1+Q_1)+g_2(P_2+Q_2)} + \frac{g_2}{1+g_1Q_1+g_2Q_2}\\ &-\frac{h_2}{1+h_2Q_2} - (\lambda_2 - \nu_2) = 0\end{aligned} \tag{97}$$

As in Section 8, we note that (94)-(97) are only necessary conditions for the optimal power allocations P_1, P_2, Q_1, and Q_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave in (P_1, P_2, Q_1, Q_2) in general. Therefore, we give power control policies P_1, P_2, Q_1, and Q_2 that satisfy these necessary conditions. That is, we obtain one fixed point (P_1, P_2, Q_1, Q_2) of the Lagrangian such that (P_1, P_2, Q_1, Q_2) satisfies the constraints (90)-(91). The power allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (94)-(97) and (90)-(91) is described in detail in Appendix B.

10 Numerical Results

In this section, we present some simple simulation results. We also plot the sum secrecy rate achieved using our SBA and ESA schemes, as well as the i.i.d. Gaussian signaling with cooperative jamming (GS/CJ) scheme in [16]. First, the secrecy sum rates achieved by the SBA and the ESA schemes scale with SNR. Hence, these rates exceed the one achieved by the GS/CJ scheme for high SNR. Second, the secrecy sum rate achieved by the ESA scheme is larger than the one achieved by the SBA scheme for all SNR.

In our first set of simulations, we use a rudimentary power allocation policy for our SBA and ESA schemes. For the SBA scheme, we first note, from (30), that the secrecy sum rate achieved can be expressed as a nested expectation as

$$\begin{aligned} R_s =& \frac{1}{2} E_{\mathbf{h}_o,\mathbf{g}_o}\Bigg\{ E_{\mathbf{h}_e,\mathbf{g}_e}\Bigg[\log\Bigg(1+\left(|h_{1o}g_{2o}|^2+|h_{1e}g_{2e}|^2\right)P_1+\left(|h_{2o}g_{1o}|^2+|h_{2e}g_{1e}|^2\right)P_2 \\ & \qquad\qquad\qquad + |h_{1e}h_{2o}g_{1o}g_{2e}-h_{1o}h_{2e}g_{1e}g_{2o}|^2P_1P_2\Bigg) \\ & \qquad\qquad - \log\Bigg(1+\left(|g_{1o}g_{2o}|^2+|g_{1e}g_{2e}|^2\right)(P_1+P_2)\Bigg)\Bigg]\Bigg\} \end{aligned} \tag{98}$$

where $\mathbf{h}_o = [h_{1o}\ h_{2o}]^T$, $\mathbf{h}_e = [h_{1e}\ h_{2e}]^T$, $\mathbf{g}_o = [g_{1o}\ g_{2o}]^T$, and $\mathbf{g}_e = [g_{1e}\ g_{2e}]^T$. For those channel gains $\mathbf{h}_o, \mathbf{g}_o$ for which the inner expectation with respect to $\mathbf{h}_e, \mathbf{g}_e$ is negative, we set $P_1 = P_2 = 0$. Otherwise, we set $P_1 = \frac{1}{2\sigma_g^2}\bar{P}_1$ and $P_2 = \frac{1}{2\sigma_g^2}\bar{P}_2$. Note that turning off the powers for some values of the channel gains $\mathbf{h}_o, \mathbf{g}_o$ is possible since P_1 and P_2 are functions of $\mathbf{h}_o$ and $\mathbf{g}_o$. Secondly, note that, if a power allocation satisfies the average power constraints, then the modified power allocation where the powers are turned off at some channel states, also satisfies the power constraints. For the ESA scheme, we first note, from (39), that the achievable secrecy sum rate is

$$R_s =\frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+2|h_1|^2P_1\right)+\log\left(1+2|h_2|^2P_2\right)-\log\left(1+2(|g_1|^2P_1+|g_2|^2P_2)\right)\right\} \tag{99}$$

In this case, we set $P_1 = P_2 = 0$ for those values of channel gains for which the difference inside the expectation is negative. Otherwise, we set $P_1 = \bar{P}_1$ and $P_2 = \bar{P}_2$. Again, turning the powers off does not violate power constraints for a power allocation scheme which already satisfies the power constraints. For the GS/CJ scheme, we use the power allocation scheme described in [16].

In Figure 1, the secrecy sum rate achieved by each of the three schemes is plotted versus the average SNR that we define as $\frac{1}{2}(\bar{P}_1 + \bar{P}_2)$. In all simulations, we set $\sigma_{h_1}^2 = \sigma_{h_2}^2 = 1.0$, we also take $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0.75$.

Next, in Figure 2, we plot secrecy sum rates achievable with constant power allocation together with secrecy sum rates achievable with power control for the ESA scheme with and without cooperative jamming.

11 Conclusions

In this paper, we proposed two new achievable schemes for the fading multiple access wiretap channel. Our first scheme, the scaling based alignment (SBA) scheme, lets the interfering signals at the main receiver live in a two-dimensional space, while it aligns the interfering signals at the eavesdropper in a one-dimensional space. We obtained the secrecy rate region achieved by this scheme. We showed that the secrecy rates achieved by this scheme scale with SNR as 1/2 log(SNR), i.e., a total of 1/2 secure DoF is achievable in the two-user fading

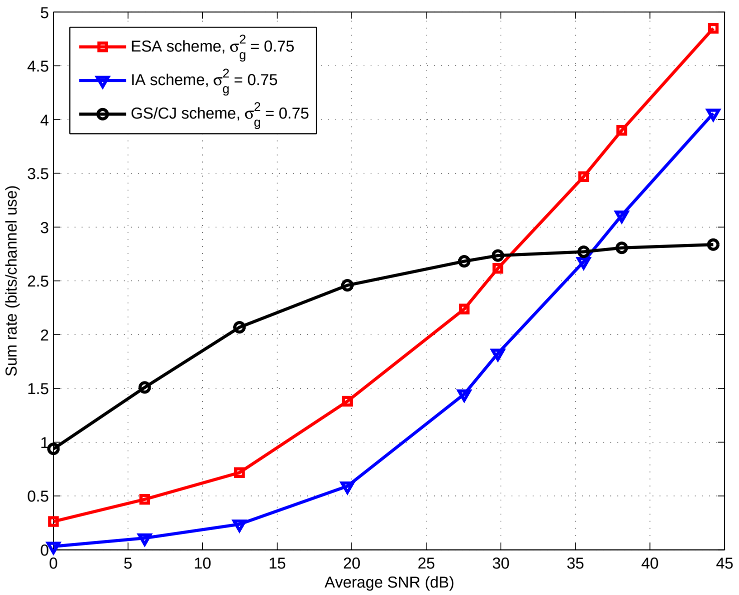

Figure 1: Achievable secrecy sum-rates of the scaling based alignment scheme (SBA scheme) of this paper, the ergodic secret alignment scheme (ESA scheme) of this paper, and the i.i.d. Gaussian signaling with cooperative jamming scheme (GS/CJ scheme) of [16], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

MAC-WT. We also showed that the secrecy sum rate achieved by the i.i.d. Gaussian signaling with cooperative jamming scheme does not scale with SNR, i.e., the achievable secure DoF is zero. As a direct consequence, we showed the sub-optimality of the i.i.d. Gaussian signaling based schemes with or without cooperative jamming in the fading MAC-WT.

Our second scheme, the ergodic secret alignment (ESA) scheme, is inspired by the ergodic interference alignment technique. In this scheme each transmitter repeats its symbols over carefully chosen time instants such that the interfering signals from the transmitters are aligned favorably at the main receiver while they are aligned unfavorably at the eavesdropper. We obtained the secrecy rate region achieved by this scheme and showed that, as in the scaling based alignment scheme, the secrecy sum rate achieved by the ergodic secret alignment scheme scales with SNR as $1/2\log(\text{SNR})$. In addition, we introduced an improved version of our ESA scheme where cooperative jamming is used as an additional ingredient to achieve higher secrecy rates. Moreover, since the rate expressions achieved with the SBA scheme seem complicated, while the rate expressions achieved with the two versions of the ESA scheme (with and without cooperative jamming) are more amenable for optimization of power allocations, we derived the necessary conditions for the optimal power allocation that maximizes the secrecy sum rate achieved by the ESA scheme when used solely and when used with cooperative jamming.

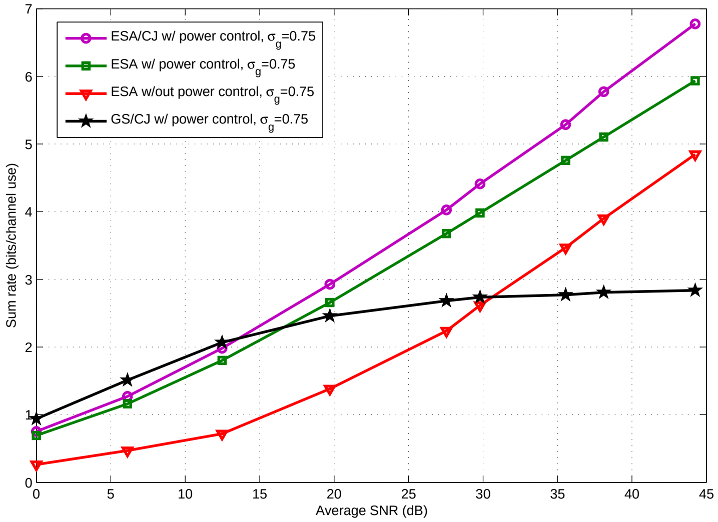

Figure 2: Achievable secrecy sum rates for the ergodic secret alignment scheme (ESA scheme) of this paper, with and without power control, the ergodic secret alignment with cooperative jamming scheme (ESA/CJ scheme) of this paper with power control, and the i.i.d. Gaussian signaling with cooperative jamming scheme (GS/CJ scheme) of [16], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

Appendices

A Power Control for the ESA Scheme

Here, we discuss the cases of the power allocation policy of Section 8.

1. $h_1 \leq \lambda_1, h_2 - g_2 \leq \lambda_2$ or $h_1 - g_1 \leq \lambda_1, h_2 \leq \lambda_2$. In this case, $P_1 = P_2 = 0$. To prove this, suppose without loss of generality that $h_1 \leq \lambda_1, h_2 - g_2 \leq \lambda_2$. We note that $h_1 \leq \lambda_1$ implies that $h_1 - \frac{g_1}{(1+g_2P_2)} \leq \lambda_1$ which, using (87), implies that $P_1 = 0$. Hence, from (88), we must also have $P_2 = 0$. In the same way, we can show that when $h_1 - g_1 \leq \lambda_1, h_2 \leq \lambda_2$, we also must have $P_1 = P_2 = 0$.

2. $h_1 \leq \lambda_1, h_2 - g_2 > \lambda_2$. In this case, $P_1 = 0$ and $P_2 > 0$ where P_2 is given by (86). As in the previous case, $h_1 \leq \lambda_1$, using (87), implies that $P_1 = 0$. Hence, from (88), we must have $P_2 > 0$.

3. $h_1 - g_1 > \lambda_1, h_2 \leq \lambda_2$. In this case, $P_1 > 0$ and $P_2 = 0$ where P_1 is given by (85). This case is the same as the previous one with roles of users 1 and 2 interchanged.

4. $\lambda_1 < h_1 \leq \lambda_1 + g_1, \lambda_2 < h_2 \leq \lambda_2 + g_2$. In this case, the solution (P_1, P_2) may not be unique. Namely, we either have $P_1 > 0$ and $P_2 > 0$, or we have $P_1 = P_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = P_2 = 0$ satisfies $h_1 - \frac{g_1}{(1+g_2P_2)} \leq \lambda_1$

and $h_2 - \frac{g_2}{(1+g_1P_1)} \leq \lambda_2$, i.e., satisfies conditions (87) and (88). It is also easy to see that we can find positive P_1 and P_2 such that $h_1 - \frac{g_1}{(1+g_2P_2)} > \lambda_1$ and $h_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2$, i.e., there exist positive P_1 and P_2 that satisfy (87) and (88). Hence the solution (P_1, P_2) may not be unique. It remains to show that we cannot have $P_1 > 0, P_2 = 0$ or $P_1 = 0, P_2 > 0$. Suppose without loss of generality that $P_1 > 0, P_2 = 0$. Hence, we have $h_1 - \frac{g_1}{(1+g_2P_2)} = h_1 - g_1 \leq \lambda_1$ which implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0, P_2 = 0$. In the same way, it can be shown that we cannot have $P_1 = 0, P_2 > 0$. Hence, we obtain our power allocation policy for this case as follows. We examine the solution of equations (83)-(84), if it yields a real and non-negative solution (P_1, P_2)[1], then we take it as our solution (P_1, P_2) for this case. Otherwise, we set $P_1 = P_2 = 0$.

5. $\lambda_1 < h_1 \leq \lambda_1 + g_1, h_2 - g_2 > \lambda_2$. In this case, we must have $P_2 > 0$. However, we either have $P_1 > 0 \quad$ or $\quad P_1 = 0$. This can be shown as follows. We note that $h_2 - g_2 > \lambda_2$ implies that $h_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2$ for any $P_1 \geq 0$. Hence, by (88), we must have $P_2 > 0$. However, we either have $P_1 > 0$ or $P_1 = 0$ depending on whether the value of P_2 satisfies $h_1 - \frac{g_1}{(1+g_2P_2)} > \lambda_1$ or not. We obtain our power allocation policies as follows. We first solve (83)-(84), if this yields a real and non-negative solution (P_1, P_2), then we take it to be the power allocation values for this case. Otherwise, we set $P_1 = 0$ and P_2 is obtained from (86).

6. $h_1 - g_1 > \lambda_1, \lambda_2 < h_2 \leq \lambda_2 + g_2$. By the symmetry between this case and the previous case, we must have $P_1 > 0$ while we either have $P_2 > 0 \quad$ or $\quad P_2 = 0$. We obtain our power allocation policies in a fashion similar to that of case 4 and case 5. In particular, we first solve (83)-(84), if this yields a real and non-negative solution (P_1, P_2), then we take it to be the power allocation values for this case. Otherwise, we set $P_2 = 0$ and P_1 is obtained from (85).

7. $h_1 - g_1 > \lambda_1, h_2 - g_2 > \lambda_2$. Here, we must have $P_1 > 0$ and $P_2 > 0$. This is due to the fact that $h_1 - g_1 > \lambda_1$ and $h_2 - g_2 > \lambda_2$ imply that $h_1 - \frac{g_1}{(1+g_2P_2)} > \lambda_1$ and $h_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2$, respectively. Hence, from (87)-(88), we must have $P_1 > 0$ and $P_2 > 0$. The values of P_1 and P_2 are given by the positive common root (P_1, P_2) of (83)-(84) which, in this case, have only one positive common root.

B Power Control for the ESA/CJ Scheme

Here, we discuss the power allocation policy of Section 9.

For each channel state, since splitting power between transmission and jamming is sub-optimal, we can distinguish between five non-zero forms that the solution (P_1, P_2, Q_1, Q_2) of

[1] Note that there is at most one such common root for these two quadratic equations.

(94)-(97) may take. First, if $P_1 > 0, P_2 > 0$ and $Q_1 = Q_2 = 0$, then $\mu_1 = \mu_2 = 0$. Hence, from (94)-(95), we conclude that (P_1, P_2) is the positive common root of equations (83)-(84) which are found in Section 8 and are rewritten here:

$$h_1 (1 + g_2 P_2) - g_1 = \lambda_1 (1 + h_1 P_1)(1 + g_1 P_1 + g_2 P_2) \tag{100}$$
$$h_2 (1 + g_1 P_1) - g_2 = \lambda_2 (1 + h_2 P_2)(1 + g_1 P_1 + g_2 P_2) \tag{101}$$

This root can be obtained through numerical solution. Secondly, if $P_1 > 0, Q_2 > 0$ and $P_2 = Q_1 = 0$, then $\mu_1 = \nu_2 = 0$. Hence, from (94) and (96), we conclude that (P_1, Q_2) is the positive common root of

$$h_1 (1 + g_2 Q_2) - g_1 = \lambda_1 (1 + h_1 P_1)(1 + g_1 P_1 + g_2 Q_2) \tag{102}$$
$$g_2 g_1 P_1 = \lambda_2 (1 + g_2 Q_2)(1 + g_1 P_1 + g_2 Q_2) \tag{103}$$

which can also be obtained through numerical solution. Thirdly, if $P_2 > 0, Q_1 > 0$ and $P_1 = Q_2 = 0$, then $\mu_2 = \nu_1 = 0$. Hence, from (95) and (97), we conclude that (P_2, Q_1) is the positive common root of

$$h_2 (1 + g_1 Q_1) - g_2 = \lambda_2 (1 + h_2 P_2)(1 + g_1 Q_1 + g_2 P_2) \tag{104}$$
$$g_1 g_2 P_2 = \lambda_1 (1 + g_1 Q_1)(1 + g_1 Q_1 + g_2 P_2) \tag{105}$$

which again can be obtained through numerical solution. The fourth non-zero form of (P_1, P_2, Q_1, Q_2) is when $P_1 > 0$ and $P_2 = Q_1 = Q_2 = 0$, then $\mu_1 = 0$. Hence, from (94), P_1 is given by (85) which is found in Section 8 and will be repeated here for convenience:

$$P_1 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{g_1} - \frac{1}{h_1}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{g_1} - \frac{1}{h_1}\right)} - \left(\frac{1}{g_1} + \frac{1}{h_1}\right)\right) \tag{106}$$

The last non-zero form of (P_1, P_2, Q_1, Q_2) is when $P_2 > 0$ and $P_1 = Q_1 = Q_2 = 0$, then $\mu_2 = 0$. Hence, from (95), P_2 is given by (86) in Section 8 and is given here again.

$$P_2 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{g_2} - \frac{1}{h_2}\right)^2 + \frac{4}{\lambda_2}\left(\frac{1}{g_2} - \frac{1}{h_2}\right)} - \left(\frac{1}{g_2} + \frac{1}{h_2}\right)\right) \tag{107}$$

We obtain the following sufficient conditions on zero jamming powers Q_1 and Q_2. By subtracting (96) from (94) and subtracting (97) from (95), we get

$$\frac{h_1}{1 + h_1 Q_1} - \frac{g_1}{1 + g_1 Q_1 + g_2 Q_2} + \mu_1 - \nu_1 = 0 \tag{108}$$
$$\frac{h_2}{1 + h_2 Q_2} - \frac{g_2}{1 + g_1 Q_1 + g_2 Q_2} + \mu_2 - \nu_2 = 0 \tag{109}$$

which, by using the fact that the two users cannot be jamming together, give the following conditions

$$Q_1 = 0, \qquad \text{if} \quad h_1 > g_1 \tag{110}$$

$$Q_2 = 0, \qquad \text{if} \quad h_2 > g_2 \tag{111}$$

Moreover, we obtain necessary and sufficient conditions for the positivity of power allocations in the possible transmission/jamming scenarios in each channel state. First, when no user jams, i.e., $Q_1 = Q_2 = 0$, then from (94)-(95), we obtain the necessary and sufficient conditions (87)-(87) of Section 8 which we repeat here for convenience.

$$P_1 > 0, \qquad \text{if and only if} \quad h_1 - \frac{g_1}{(1+g_2P_2)} > \lambda_1 \tag{112}$$

$$P_2 > 0, \qquad \text{if and only if} \quad h_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2 \tag{113}$$

Secondly, when user 1 does not jam and user 2 does not transmit, i.e., $Q_1 = P_2 = 0$, then from (94) and (96), we can easily derive the following necessary and sufficient conditions for the positivity of the transmission power P_1 of user 1 and the jamming power Q_2 of user 2.

$$P_1 > 0, \qquad \text{if and only if} \quad h_1 - \frac{g_1}{(1+g_2Q_2)} > \lambda_1 \tag{114}$$

$$Q_2 > 0, \qquad \text{if and only if} \quad g_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2 \tag{115}$$

Thirdly, when user 1 does not transmit and user 2 does not jam, i.e., $P_1 = Q_2 = 0$, then from (95) and (97), we can similarly derive the following necessary and sufficient conditions for the positivity of the transmission power P_2 of user 2 and the jamming power Q_1 of user 1.

$$P_2 > 0, \qquad \text{if and only if} \quad h_2 - \frac{g_2}{(1+g_1Q_1)} > \lambda_2 \tag{116}$$

$$Q_1 > 0, \qquad \text{if and only if} \quad g_1 - \frac{g_1}{(1+g_2P_2)} > \lambda_1 \tag{117}$$

Using conditions (110)-(117) given above, the power allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (94)-(97) and (90)-(91) can be fully described through the following cases of the channel gains.

1. $h_1 > g_1, h_2 > g_2$. In this case, we must have $Q_1 = Q_2 = 0$. This follows directly from (110)-(111). Hence, this case reduces to one of the 7 cases given in Section 8 depending on the relative values of the channel gains and the values of λ_1 and λ_2. We can obtain the power allocations P_1 and P_2 in the same way described in Section 8.

2. $h_1 > g_1, h_2 < g_2$. In this case, we must have $P_2 = Q_1 = 0$. This can be shown as follows. From (110), we must have $Q_1 = 0$. Suppose $P_2 > 0$. Hence, $\mu_2 = 0$. Since

dividing power among transmission and jamming is suboptimal, then we must have $Q_2 = 0$. Since $Q_1 = 0$, then (109) implies $\bar{h}_2 - \bar{g}_2 \geq 0$ which is a contradiction. Therefore, $P_2 = 0$. The power allocations P_1 and Q_2 are obtained from one of the following sub-cases:

(a) $h_1 \leq \lambda_1 \quad$ or $\quad h_1 - g_1 \leq \lambda_1, g_2 \leq \lambda_2$. We have $P_1 = Q_2 = 0$. To see this, note that $h_1 \leq \lambda_1$ implies that $h_1 - \frac{g_1}{(1+g_2Q_2)} \leq \lambda_1$. Hence, using (114), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $g_2 \leq \lambda_2$, then it follows from (115) that $Q_2 = 0$. Hence, the fact that $h_1 - g_1 \leq \lambda_1$ together with (114) implies that $P_1 = 0$.

(b) $h_1 - g_1 > \lambda_1, g_2 \leq \lambda_2$. We have $Q_2 = 0$ and $P_1 > 0$ where P_1 is given by (106). This can be shown to be true as follows. Since $g_2 \leq \lambda_2$, then, using (115), we must have $Q_2 = 0$. Hence, from (114) and the fact that $h_1 - g_1 > \lambda_1$ in this case, we must have $P_1 > 0$.

(c) $\lambda_1 < h_1 \leq \lambda_1 + g_1, g_2 > \lambda_2$. In this case, the solution (P_1, Q_2) may not be unique. Namely, we either have $P_1 > 0$ and $Q_2 > 0$, or we have $P_1 = Q_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = Q_2 = 0$ satisfies $h_1 - \frac{g_1}{(1+g_2Q_2)} \leq \lambda_1$ and $g_2 - \frac{g_2}{(1+g_1P_1)} \leq \lambda_2$, i.e. conditions (114) and (115). It is also easy to see that we can find positive P_1 and Q_2 that satisfy $h_1 - \frac{g_1}{(1+g_2Q_2)} > \lambda_1$ and $g_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_2$, i.e. conditions (114) and (115). Hence the solution (P_1, Q_2) may not be unique. It remains to show that we cannot have $P_1 > 0, Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $h_1 - \frac{g_1}{(1+g_2Q_2)} = h_1 - g_1 \leq \lambda_1$ which, by (114), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. We obtain our power allocation policies for this case as follows. We examine the solution of equations (102) and (103), if it yields a real and non-negative solution (P_1, Q_2), then we take it as our solution (P_1, Q_2) for this case. Otherwise, we set $P_1 = Q_2 = 0$.

(d) $h_1 - g_1 > \lambda_1, g_2 > \lambda_2$. Here, we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$, i.e., the solution may not be unique. To see this, we note that $h_1 - g_1 > \lambda_1$ implies that $h_1 - \frac{g_1}{(1+g_2Q_2)} > \lambda_2$ for any $Q_2 \geq 0$. Hence, by (114), we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$ depending on whether the value of P_1 satisfies $g_2 - \frac{g_2}{(1+g_1P_1)} > \lambda_1$ or not. We obtain our power allocation policy as follows. We first solve (102) and (103), if this yields a real and non-negative solution (P_1, Q_2), then we take it to be the power allocation values for this case. Otherwise, we set $Q_2 = 0$ and P_1 is obtained from (106).

3. $h_1 < g_1, h_2 > g_2$. From the symmetry between this case and the previous case, the power allocation roles can be obtained in this case by interchanging the power allocation

roles of users 1 and 2 in the previous case. In particular, we must have $P_1 = Q_2 = 0$. The power allocations P_2 and Q_1 are given by one of the following sub-cases:

(a) $h_2 \leq \lambda_2 \quad \text{or} \quad g_1 \leq \lambda_1, h_2 - g_2 \leq \lambda_2$. We have $P_2 = Q_1 = 0$.

(b) $g_1 \leq \lambda_1, h_2 - g_2 > \lambda_2$. We have $Q_1 = 0$ and $P_2 > 0$ where P_2 is given by (107).

(c) $g_1 > \lambda_1, \lambda_2 < h_2 \leq \lambda_2 + g_2$. In this case, the solution (P_2, Q_1) may not be unique as we either have $P_2 > 0$ and $Q_1 > 0$, or have $P_1 = Q_2 = 0$. Therefore, we obtain our power allocation policy for this case by numerically solving equations (104) and (105), if we have a real and non-negative solution (P_2, Q_1), then we take it as to be the power allocation values for this case. Otherwise, we set $P_2 = Q_1 = 0$.

(d) $g_1 > \lambda_1, h_2 - g_2 > \lambda_2$. Here, we must have $P_2 > 0$. However, we either have $Q_1 > 0$ or $Q_1 = 0$, i.e., the solution may not be unique. We obtain our power allocation policy as follows. We first solve (104)-(105), if this yields a real and non-negative solution (P_2, Q_1), then we take it to be the power allocation values for this case. Otherwise, we set $Q_1 = 0$ and P_2 is obtained from (107).

4. $h_1 < g_1, h_2 < g_2$. In this case, we have $P_2 = Q_1 = 0$ or $P_1 = Q_2 = 0$. In order to see this, suppose $P_1 > 0$ and $P_2 > 0$. Hence, $\mu_1 = \mu_2 = 0$. Since splitting a user's power into transmit and jamming powers is suboptimal, then we must have $Q_1 = Q_2 = 0$. Thus, from (108) and (109), we have $\bar{h}_1 \geq \bar{g}_1$ and $\bar{h}_2 \geq \bar{g}_2$ which is a contradiction. Therefore, we must have either $P_1 = 0$ or $P_2 = 0$. The power allocation policy (P_1, P_2, Q_1, Q_2) is given in the following four sub-cases of channel states:

   (a) $(h_1 \leq \lambda_1 \quad \text{or} \quad g_2 \leq \lambda_2)$ and $(h_2 \leq \lambda_2 \quad \text{or} \quad g_1 \leq \lambda_1)$. In this case, we have $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$. We note that if $h_1 \leq \lambda_1$ then $h_1 - \frac{g_1}{(1+g_2Q_2)} \leq \lambda_1$. Hence, using (114), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $g_2 \leq \lambda_2$, then it follows from (115) that $Q_2 = 0$. Hence, the fact that $h_1 < g_1$ together with (114) implies that $P_1 = 0$. Next, suppose that $P_1 = Q_2 = 0$. Using the fact that $h_2 \leq \lambda_2$ or $g_1 \leq \lambda_1$ together with condition (116)-(117), we can show that $P_2 = Q_1 = 0$. Therefore, in this case, we must have $P_1 = P_2 = Q_1 = Q_2 = 0$.

   (b) $(h_2 \leq \lambda_2 \quad \text{or} \quad g_1 \leq \lambda_1)$ and $(h_1 > \lambda_1, g_2 > \lambda_2)$. We have $P_2 = Q_1 = 0$. The solution (P_1, Q_2) may not be unique. In particular, we may have $P_1 > 0, Q_2 > 0$ or have $P_1 = Q_2 = 0$. To see this, consider the following argument. Using the fact that $h_2 \leq \lambda_2$ or $g_1 \leq \lambda_1$, then, as shown in case 4(a), we conclude that we must have $P_2 = Q_1 = 0$. Now, we consider the power allocation policy (P_1, Q_2). We note that $P_1 = Q_2 = 0$ satisfies conditions (114) and (115). On the other hand, we can find positive P_1 and Q_2 that satisfy (114) and (114). Hence, the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0, Q_2 > 0$.

It remains to show that we cannot have $P_1 > 0, Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $h_1 - \frac{g_1}{(1+g_2Q_2)} = h_1 - g_1 < 0 < \lambda_1$ which, by (114), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. Our power allocations P_1 and Q_2 are obtained for this case as follows. We solve (102) and (103). If the solution gives a real and non-negative common root (P_1, Q_2), we take it as our power allocation values for P_1 and Q_2. Otherwise, we set $P_1 = Q_2 = 0$.

(c) $(h_1 \leq \lambda_1 \quad \text{or} \quad g_2 \leq \lambda_2)$ and $(h_2 > \lambda_2, g_1 > \lambda_1)$. By the symmetry between this case and case $4(b)$, we have $P_1 = Q_2 = 0$. Again in this case, the solution (P_2, Q_1) may not be unique. In particular, we may have $P_2 > 0, Q_1 > 0$ or have $P_2 = Q_1 = 0$. In fact, the power allocation policy in this case, can be obtained from case $4(b)$ by interchanging the roles of users 1 and 2. Our power allocations P_2 and Q_1 are obtained as follows in this case. We solve (104)-(105). If the solution gives a real and non-negative common root (P_2, Q_1), we take it as our power allocation values for P_2 and Q_1. Otherwise, we set $P_2 = Q_1 = 0$.

(d) $(h_1 > \lambda_1, g_2 > \lambda_2)$ and $(h_2 > \lambda_2, g_1 > \lambda_1)$. Here, again the solution (P_1, P_2, Q_1, Q_2) is not unique as we may either have $P_1 > 0, Q_2 > 0, P_2 = Q_1 = 0$, or $P_2 > 0, Q_1 > 0, P_1 = Q_2 = 0$, or $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$ and consider the power allocation policy (P_1, Q_2). As in case $4(b)$, we can show that the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0, Q_2 > 0$. However, as shown in case $4(b)$, we cannot have $P_1 > 0, Q_2 = 0$. Next, suppose that $P_1 = Q_2 = 0$ and consider the power allocation policy (P_2, Q_1). As in case $4(c)$, we can show that the solution (P_2, Q_1) may not be unique as we may have $P_2 = Q_1 = 0$ or $P_2 > 0, Q_1 > 0$. However, we cannot have $P_2 > 0, Q_1 = 0$. We obtain our allocation policy (P_1, P_2, Q_1, Q_2) as follows. Let us denote the solution of (102) and (103) together by *solution* A and denote the solution of (104) and (105) together by *solution* B.

i. If solution A yields a real non-negative (P_1, Q_2) while solution B does not yield real non-negative (P_2, Q_1), then we take (P_1, Q_2) to be the power allocation values for users 1 and 2, respectively, and set $P_2 = Q_1 = 0$.

ii. If solution B yields a real non-negative (P_2, Q_1) while solution A does not yield real non-negative (P_1, Q_2), then we take (P_2, Q_1) to be the power allocation values for users 2 and 1, respectively, and set $P_1 = Q_2 = 0$.

iii. If neither solution A nor solution B gives real non-negative common root, then we set $P_1 = P_2 = Q_1 = Q_2 = 0$.

iv. If both solutions A and B yield a real non-negative common root, then we either choose the root given by solution A, i.e., (P_1, Q_2), and set $P_2 = Q_1 = 0$, or choose the root given by solution B, i.e., (P_2, Q_1), and set $P_1 = Q_2 = 0$.

We make the choice that maximizes the achievable *instantaneous* secrecy sum rate.

References

[1] R. Bassily and S. Ulukus. A new achievable ergodic secrecy rate region for the fading multiple access wiretap channel. In *47th Annual Allerton Conference on Communications, Control and Computing, Monticello, IL*, Sep. 2009.

[2] R. Bassily and S. Ulukus. Ergodic secret alignment for the fading multiple access wiretap channel. In *IEEE International Conference on Communications, Cape Town, South Africa*, May 2010.

[3] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[4] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[5] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Inf. Theory*, 24(3):339–348, May 1978.

[6] S. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Inf. Theory*, 24(4):451–456, Jul. 1978.

[7] E. Tekin and A. Yener. The Gaussian multiple access wiretap channel. *IEEE Trans. on Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[8] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[9] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*. W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[10] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *46th Annual Allerton Conference on Communication, Control and Computing*, Sep. 2008.

[11] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Trans. on Inf. Theory*, Oct. 2008. Submitted. Also available at [arXiv:0810.1187v1].

[12] T. Gou and S. A. Jafar. On the secure degrees of freedom of wireless X networks. In *46th Annual Allerton Conference on Communication, Control and Computing, UIUC, IL*, pages 826–833, Sep. 2008.

[13] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. In *IEEE Globecom*, 2009. Also available at [arXiv:0905.2638].

[14] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. In *IEEE ITW'09, Volos*, Jun. 2009.

[15] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees of freedom of the multiple access channel. In *IEEE International Symposium on Inf. Theory ISIT, Austin, TX*, Jun. 2010. Also available at [arXiv:1003.0729].

[16] E. Tekin and A. Yener. Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading. In *45th Annual Allerton Conference on Communication, Control and Computing*, pages 856–863, Sep. 2007.

[17] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath. Ergodic interference alignment. In *IEEE ISIT, Seoul, Korea*, Jun. 2009.